(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
7 août 2003 (07.08.2003)

PCT

(10) Numéro de publication internationale
WO 03/065681 A1

(51) Classification internationale des brevets[7] :
H04L 29/06, 29/08

(21) Numéro de la demande internationale :
PCT/FR03/00288

(22) Date de dépôt international :
31 janvier 2003 (31.01.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/01435 1 février 2002 (01.02.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **TRUSTED LOGIC** [FR/FR]; 5, rue du Bailliage, F-78000 Versailles (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **VETILLARD, Eric** [FR/FR]; 1, Passage des Pignes, F-06560 Valbonne (FR).

(74) Mandataire : **PONCET, Jean-François**; Cabinet Poncet, 7, chemin de Tillier, B.P. 317, F-74008 Annecy Cedex (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

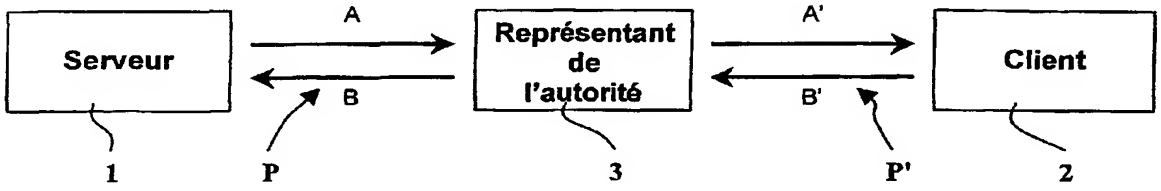
(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :
— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR SECURING MESSAGES EXCHANGED IN A NETWORK

(54) Titre : PROCEDE ET DISPOSITIF POUR SECURISER LES MESSAGES ECHANGES SUR UN RESEAU



1 SERVER
2 CLIENT
3 REPRESENTATIVE OF THE AUTHORITY

(57) **Abstract:** In order to secure messages that are exchanged in a data transmission network between a server (1) and a client (2), a control device that is decentralized or represents the authority (3) is permanently inserted into the network between the server (1) and the user (2) during the secured exchange of messages. Said representative of the authority (3) translates the transmitted messages and carries out the message verifications that have been decided by the authority. Said representative of the authority (3) can be a specific microprocessor card, for example, which is permanently inserted between the server (1) and the client (2), whereby the authority does not need to be directly involved in the transactions and no permanent connection with the authority is required.

(57) **Abrégé :** Pour sécuriser les messages échangés sur un réseau de transmissions de données entre un serveur (1) et un client (2), on intercale un dispositif de contrôle décentralisé ou représentant de l'autorité (3) en permanence dans le réseau entre le serveur (1) et le client (2) pendant l'échange sécurisé des messages. Le représentant de l'autorité (3) effectue une traduction des messages transmis, et effectue sur les messages tranmis les contrôles décidés par l'autorité. Ce représentant de l'autorité (3) peut par exemple être une carte à microprocesseur spécifique, intercalée en permanence entre le serveur (1) et le client (2). L'autorité peut donc ne pas être directement dans les transactions, et il n'est pas besoin d'une connexion permanence avec l'autorité.

WO 03/065681 A1

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE ET DISPOSITIF POUR SECURISER LES MESSAGES ECHANGES SUR UN RESEAU

DOMAINE TECHNIQUE DE L'INVENTION

La présente invention concerne les systèmes d'information à réseau de transmission de données dans lesquels la communication entre un serveur et un client s'effectue par l'intermédiaire du réseau sous le contrôle d'une autorité qui définit des règles concernant cette communication.

Le contrôle effectif des communications par l'autorité nécessite de contacter directement l'autorité en permanence, ce qui exige une connexion permanente à distance.

Le contrôle effectif de la communication par l'autorité est souvent difficile à mettre en œuvre, en particulier dans des situations où l'autorité ne peut être directement contactée, dans des situations où l'autorité ne souhaite pas être directement impliquée dans une transaction, ou dans des situations où le client et le serveur ne peuvent pas entrer directement en contact.

EXPOSE DE L'INVENTION

Le problème proposé par l'invention est de concevoir une nouvelle architecture de système d'information à réseau, dans laquelle un contrôle puisse être exécuté par une autorité sans nécessiter une connexion permanente avec l'autorité.

On cherche simultanément à s'assurer que le contrôle est réalisé en permanence, de sorte que les transmissions soient correctement sécurisées.

L'idée qui est à la base de l'invention est d'assurer le contrôle effectif et permanent de la communication par un représentant de l'autorité qui est implémenté dans ou à proximité immédiate du client, de sorte que l'invention peut s'appliquer à des architectures dans lesquelles le client est de petite taille et ne comporte pas en lui-même les ressources nécessaires pour remplir les fonctions de sécurité et les autres fonctions de représentant de l'autorité.

Pour atteindre ces buts ainsi que d'autres, l'invention prévoit un procédé pour sécuriser les messages échangés sur un réseau de transmission de données entre un serveur et un client, sous le contrôle d'une autorité qui définit les règles d'échange

des messages ; selon l'invention le contrôle est assuré de manière décentralisée par un représentant de l'autorité, intercalé en permanence dans le réseau entre le serveur et le client, à proximité du client, pendant l'échange sécurisé des messages, effectuant une traduction des messages transmis et effectuant sur les messages transmis les contrôles décidés par l'autorité.

Selon un mode de réalisation avantageux, on utilise un premier protocole pour les échanges entre le serveur et le représentant de l'autorité, et on utilise un second protocole différent du premier protocole pour les échanges entre le représentant de l'autorité et le client.

En pratique, pour l'échange de messages selon l'invention :

- on établit entre le serveur et le représentant de l'autorité un premier canal sécurisé en utilisant une première clé connue du représentant de l'autorité et du serveur mais pas du client, et en utilisant un premier algorithme de cryptage,
- on établit entre le représentant de l'autorité et le client un second canal sécurisé en utilisant une seconde clé connue du représentant de l'autorité et du client mais pas du serveur, et en utilisant un second algorithme de cryptage.

L'invention prévoit également un dispositif pour sécuriser les messages échangés sur un réseau de transmission de données entre un serveur et un client sous le contrôle d'une autorité qui définit les règles d'échange des messages ; selon l'invention on prévoit un dispositif de contrôle décentralisé ou représentant de l'autorité, intercalé en permanence dans le réseau entre le serveur et le client, à proximité du client, pendant l'échange sécurisé des messages, effectuant une traduction des messages transmis, et effectuant sur les messages transmis les contrôles décidés par l'autorité.

Selon un mode de réalisation avantageux, le dispositif de contrôle décentralisé ou représentant de l'autorité est un microsystème informatique matériellement sécurisé, intercalé en permanence entre le serveur et le client pendant l'échange sécurisé des messages.

On peut avantageusement prévoir que :

- le serveur est un système informatique comprenant un port d'entrée-sortie ;
- le client est un microsystème informatique comprenant un port d'entrée-sortie ;
- le représentant de l'autorité est un microsystème informatique matériellement sécurisé comprenant un dispositif d'interface ;
- un système spécifique d'interfaçage est prévu, comprenant un port d'entrée-sortie connecté au port d'entrée-sortie du système informatique serveur, comprenant un port de cartes connecté au port d'entrée-sortie du microsystème informatique client, comprenant un port d'entrée-sortie connecté au dispositif d'interface du microsystème informatique représentant l'autorité, et comprenant un contrôleur programmé pour contrôler les communications entre les ports d'entrée-sortie ;
- le contrôleur et le représentant de l'autorité sont programmés de façon que :
  - le système informatique serveur envoie une requête A au microsystème informatique client, et cette requête est reçue par le contrôleur ;
  - le contrôleur transmet la requête A au représentant de l'autorité, qui lui retourne une réponse Ra ;
  - cette réponse Ra est utilisée par le contrôleur pour calculer une requête A' qui est envoyée au microsystème informatique client ;
  - la requête A' est traitée par le microsystème informatique client, qui prépare une réponse B' ;
  - le microsystème informatique client envoie la réponse B' au système informatique serveur ; cette réponse est reçue par le contrôleur ;
  - le contrôleur transmet la réponse B' au représentant de l'autorité, qui lui retourne une réponse Rb ;
  - cette réponse Rb est utilisée par le contrôleur pour calculer une réponse B qui est envoyée au système informatique serveur.

Selon une première application, on peut prévoir que :

- le client est une carte à microprocesseur ;
- le représentant de l'autorité est une carte à microprocesseur ;

- le système spécifique d'interfaçage est un lecteur de cartes à microprocesseur comportant deux ports de cartes.

Selon une seconde application, on peut prévoir que :

- le client est un système mobile de communication ;
- le serveur est un système informatique communiquant avec le client par une connexion physique ou par un réseau de communication sans fil ;
- le représentant de l'autorité est une carte à microprocesseur représentant l'opérateur du réseau de communication sans fil (dite carte SIM dans les téléphones répondant aux normes GSM).

Selon une troisième application, on peut prévoir que :

- le client est une carte à microprocesseur ;
- le représentant de l'autorité est un système informatique matériellement sécurisé ;
- le système spécifique d'interfaçage est une machine comportant un port de cartes et une interface d'entrée-sortie spécifique de liaison avec le système informatique représentant de l'autorité.

DESCRIPTION SOMMAIRE DES DESSINS

D'autres objets, caractéristiques et avantages de la présente invention ressortiront de la description suivante de modes de réalisation particuliers, faite en relation avec les figures jointes, parmi lesquelles:

- la figure 1 illustre schématiquement l'échange des messages entre le serveur et le client selon la solution générale de la présente invention ;
- la figure 2 illustre l'échange des messages entre serveur et client, dans l'application au téléchargement d'un code exécutable ;
- la figure 3 illustre la transmission de messages du serveur vers le client dans une application de cryptographie à clé publique ;
- la figure 4 illustre un mode de réalisation de l'invention où le serveur est un système informatique, et le client est une carte à microprocesseur, connectée au système informatique par le biais d'un lecteur de cartes à microprocesseur ;
- la figure 5 illustre un mode de réalisation selon la figure 4, et où le représentant de l'autorité est implémenté dans une autre carte à microprocesseur connectée au même lecteur de cartes ;

- la figure 6 illustre le flux de la requête envoyée du serveur au client dans le mode de réalisation de la figure 5 ; et
- la figure 7 illustre le flux de la réponse envoyée du client au serveur dans le mode de réalisation de la figure 5.

DESCRIPTION DES MODES DE REALISATION PREFERES

Comme illustré de façon générale sur la figure 1, un dispositif pour sécuriser les messages échangés sur un réseau de transmission de données entre un serveur 1 et un client 2, sous le contrôle d'une autorité qui définit les règles d'échange des messages, comprend un dispositif de contrôle décentralisé, constitué par un représentant de l'autorité 3, intercalé en permanence dans le réseau entre le serveur 1 et le client 2 pendant l'échange sécurisé de messages.

Le représentant de l'autorité 3 effectue une traduction des messages, ainsi que des actions décidées par l'autorité.

Du point de vue des protocoles, ce représentant de l'autorité 3 est entièrement transparent, dans la mesure où le serveur 1 communique avec lui comme avec un de ses clients, et le client 2 communique avec lui comme avec un serveur.

Par contre, il est dès lors possible d'avoir des protocoles différents, soit un premier protocole P entre le serveur 1 et le représentant de l'autorité 3, et un second protocole P' entre le représentant de l'autorité 3 et le client 2. Le message A transmis par le serveur 1 est transformé par le représentant de l'autorité 3 en un message A' reçu par le client 2. En retour, le message de réponse B' émis par le client 2 est transformé par le représentant de l'autorité 3 en un message B reçu par le serveur 1.

Le représentant de l'autorité 3, réalisant un dispositif de contrôle décentralisé, peut avantageusement être disposé à proximité du client 2.

Une solution avantageuse consiste à implémenter le représentant de l'autorité 3 dans une carte à microprocesseur spécifique, intercalée en permanence entre le serveur 1 et le client 2 pendant l'échange sécurisé de messages.

Le représentant de l'autorité 3 détient des secrets appartenant à l'autorité, qui permettent d'assurer qu'une communication entre le serveur 1 et le client 2 ne peut être

établie que sous son contrôle. Un protocole cryptographique peut avantageusement être utilisé pour s'assurer de l'utilisation du représentant de l'autorité 3.

Dans le cas où le représentant de l'autorité 3 est implémenté dans une carte à microprocesseur, cela permet de s'assurer que les secrets détenus par ce représentant de l'autorité 3 sont abrités d'attaques extérieures.

On décrira maintenant un premier exemple d'utilisation de l'invention, pour la vérification d'un code exécutable devant être téléchargé dans le client 2. Cette application est décrite en relation avec la figure 2.

Un serveur 1 peut être amené dans certains cas à télécharger du code exécutable dans un client 2. Toutefois, ce code doit répondre à un ensemble de propriétés qui doivent être vérifiées par une autorité de vérification avant d'autoriser ce chargement. Ces vérifications sont destinées à assurer la sécurité du client, et sont donc généralement sous la responsabilité du propriétaire du client.

L'invention s'adresse au cas où le client 2 est un microsystème informatique tel qu'une carte à microprocesseur ou un autre système embarqué aux capacités sécuritaires limitées, par exemple un téléphone cellulaire ou un assistant numérique personnel. Le chargement de programmes doit s'effectuer par le biais d'un canal sécurisé entre le serveur et le client, canal sécurisé qui permet de garantir l'intégrité et/ou la confidentialité des informations transmises sur le canal. L'établissement de ce canal nécessite l'existence d'un secret cryptographique partagé (clé K) entre le client 2 et le serveur 1.

Selon l'invention, on peut utiliser une carte à microprocesseur spécifique, qui représente l'autorité de vérification et constitue le représentant de l'autorité 3. La carte à microprocesseur est intercalée entre le serveur 1 et le client 2. Ce représentant de l'autorité 3 peut alors effectuer toutes les vérifications nécessaires. Il établit deux canaux sécurisés pour l'échange des messages :

- entre le serveur 1 et le représentant de l'autorité 3, un premier canal sécurisé 4 en utilisant une première clé Ks connue du

représentant de l'autorité 3 et du serveur 1 mais pas du client 2, et en utilisant un premier algorithme de cryptage AL,

- entre le représentant de l'autorité 3 et le client 2 un second canal sécurisé 5 en utilisant une seconde clé Kc connue du représentant de l'autorité 3 et du client 2 mais pas du serveur 1, et en utilisant un second algorithme de cryptage AL'.

Cela permet d'assurer que la communication entre le client 2 et le serveur 1 ne peut être établie qu'à travers le représentant de l'autorité 3, et donc que les vérifications nécessaires sont effectuées.

Un chargement de code peut alors s'effectuer de la manière suivante :

- le serveur 1 établit un premier canal sécurisé 4 avec le représentant de l'autorité 3, en utilisant la clé Ks et l'algorithme AL ;
- le serveur 1 envoie le code à charger C au représentant de l'autorité 3, par le biais du premier canal sécurisé 4 ; on note sur la figure 2 l'indication C(AL)Ks pour indiquer que le code C est sécurisé par l'algorithme AL et la clé Ks (signature et/ou chiffrement) ;
- le représentant de l'autorité 3 vérifie les propriétés sur le code C ; on dénote par VC le code ainsi vérifié, auquel il peut être ajouté une preuve que la vérification a bien été effectuée ;
- le représentant de l'autorité 3 établit un second canal sécurisé 5 avec le client 2, en utilisant la clé Kc et l'algorithme AL' ;
- le représentant de l'autorité 3 envoie le code vérifié VC au client 2 en utilisant le second canal sécurisé 5 établi ci-dessus ; il transmet donc VC(AL')Kc ;
- si nécessaire, le client 2 renvoie une preuve de chargement P par le biais du second canal sécurisé 5 : il envoie donc P(AL')Kc ; le représentant de l'autorité 3 traduit alors ce message en utilisant P(AL)Ks pour communiquer avec le serveur 1.

Cette solution comporte de nombreux avantages : la vérification peut être effectuée de manière systématique, sans toutefois nécessiter une communication directe avec l'autorité de vérification ; et la vérification peut être effectuée sans nécessiter aucun changement du client ou du serveur : pour le

serveur 1, le représentant de l'autorité 3 se comporte comme un client ; pour le client 2, le représentant de l'autorité 3 se comporte comme un serveur.

En outre, la solution selon l'invention ne nécessite pas de ressource supplémentaire dans le client 2 pour effectuer la vérification. Elle ne nécessite pas, non plus, que le client 2 soit en mesure de vérifier des signatures électroniques. Egalement, la solution assure une grande flexibilité. Enfin, la solution permet une implantation dans une carte à microprocesseur, qui peut ainsi fonctionner dans des environnements non connectés.

On décrira maintenant un second exemple d'application de l'invention à la cryptographie à clé publique.

Certains protocoles cryptographiques utilisés avec des cartes à microprocesseur sont basés sur l'utilisation de cryptographie à clés publiques. Toutefois, ces techniques cryptographiques sont coûteuses, et ne sont donc pas supportées par toutes les cartes à microprocesseur.

Un cas particulièrement intéressant réside dans la vérification de signatures électroniques permettant par exemple de garantir l'origine d'une donnée téléchargée. Ces signatures électroniques sont généralement implémentées à l'aide d'algorithmes à clé publique. Mais cela pose un problème aux cartes à microprocesseur les plus simples, et à d'autres systèmes simples, à cause des ressources importantes nécessaires pour utiliser l'algorithme. Ces algorithmes reposent sur une paire de clés (Kpriv, Kpub). La clé Kpriv est utilisée par le serveur 1 pour calculer la signature de la données, et ne doit être connue que du seul serveur 1. La clé Kpub est utilisée pour vérifier la signature de la donnée par le client 2, et elle peut être diffusée sans contrainte de confidentialité.

Selon l'invention on intercale, entre le serveur 1 qui envoie la donnée à signature électronique et le client 2 qui reçoit la donnée et vérifie la signature électronique, un représentant de l'autorité 3 de contrôle du client 2. Ce représentant de l'autorité 3 sera chargé de vérifier la signature électronique au nom du client 2 et ensuite de lui communiquer la donnée par le biais d'un

canal sécurisé par une clé Kc, connue uniquement du représentant de l'autorité 3 et du client 2.

Le processus de communication est illustré sur la figure 3 :

- le serveur 1 calcule la signature de la donnée D avec la clé Kpriv et l'algorithme AL. Le résultat est D(AL)Kpriv ;
- le serveur 1 communique la donnée D et la signature au représentant de l'autorité 3, éventuellement par le biais d'un premier canal sécurisé 4 ;
- le représentant de l'autorité 3 vérifie la signature et la donnée D ;
- le représentant de l'autorité 3 établit un second canal sécurisé 5 avec le client 2 au moyen de la clé Kc et de l'algorithme AL' ;
- le représentant de l'autorité 3 transmet la donnée D sous la forme D(AL')Kc, sans la signature, au client 2 par le biais du second canal sécurisé 5.

Contrairement au premier exemple précédent, le représentant de l'autorité 3 n'est pas entièrement transparent, dans la mesure où le protocole utilisé entre le serveur 1 et le représentant de l'autorité 3 diffère du protocole utilisé entre le représentant de l'autorité 3 et le client 2. Cette solution peut d'ailleurs être utilisée dans d'autres cas où des traductions de protocole sont nécessaires.

Dans les exemples ci-dessus, l'utilisation d'un représentant de l'autorité 3 est rendue transparente pour le serveur 1 et pour le client 2 d'un point de vue logique, mais les messages doivent toutefois être acheminés physiquement vers le représentant de l'autorité 3 au lieu d'être acheminés vers le client 2. Il est donc nécessaire que le serveur 1 soit programmé pour communiquer avec le représentant de l'autorité 3, et non pas pour communiquer avec le client 2.

Dans les cas où le serveur 1 est classiquement programmé pour communiquer directement avec le client 2, et où le serveur 1 est un système informatique et le client 2 est une carte à microprocesseur, l'invention propose par exemple d'intégrer le mécanisme de représentant de l'autorité 3, soit de façon permanente dans un lecteur de cartes à microprocesseur 7 connectant le système

informatique serveur 1 à la carte cliente 2, comme illustré sur la figure 4, soit de façon amovible dans une carte à microprocesseur distincte connectée au lecteur de carte à microprocesseur 7, comme illustré sur la figure 5. Dans ce mode de réalisation de la figure 5, le système informatique serveur 1 comprend un port d'entrée-sortie 1a. Le système informatique serveur 1 est associé au lecteur de cartes à microprocesseur 7 qui comprend un port d'entrée-sortie 8 connecté au port d'entrée-sortie 1a du système informatique serveur 1. Le lecteur de cartes à microprocesseur 7 comprend un port de cartes 10 adapté pour connecter une carte à microprocesseur 3 représentant l'autorité, et un port de cartes 9 adapté pour connecter une carte à microprocesseur 2, le client dans cette réalisation. La carte à microprocesseur 2 comprend un port d'entrée-sortie 12 connecté au port de cartes 9. Le lecteur de cartes à microprocesseur 7 comprend également un contrôleur 11 programmé pour contrôler les communications entre le port d'entrée-sortie 8, le port de cartes 10, et le port de cartes 9.

La carte à microprocesseur 3 connectée au port de cartes 10 définit ainsi un représentant de l'autorité.

Le contrôleur 11, et la carte à microprocesseur 3 (le représentant de l'autorité) sont programmés de façon que les flux de données se déroulent comme illustré sur la figure 6 pour une requête envoyée du système informatique serveur 1 vers la carte à microprocesseur cliente 2, et comme illustré sur la figure 7 pour une réponse retournée de la carte à microprocesseur cliente 2 vers le système informatique serveur 1.

Pour le flux de la requête envoyée du système informatique serveur 1 vers la carte à microprocesseur cliente 2 (figure 6):

- le système informatique serveur 1 envoie une requête A à la carte à microprocesseur cliente 2. Cette requête est reçue par le contrôleur 11 ;
- le contrôleur 11 transmet la requête A au représentant de l'autorité 3, qui lui retourne une réponse Ra ;
- cette réponse Ra est utilisée par le contrôleur 11 pour calculer une requête A' qui est envoyée à la carte à microprocesseur cliente 2.

Le flux de réponse retourné par la carte à microprocesseur cliente 2 au système informatique serveur 1 se déroule de la façon suivante (figure 7):

- la carte à microprocesseur cliente 2 envoie une réponse B' au système informatique serveur 1. Cette réponse est reçue par le contrôleur 11 ;
- le contrôleur 11 transmet la réponse B' au représentant de l'autorité 3, qui lui retourne une réponse Rb ;
- cette réponse Rb est utilisée par le contrôleur 11 pour calculer une réponse B qui est envoyée au système informatique serveur 1.

Dans le cas le plus simple, les réponses Ra et Rb peuvent être une simple encapsulation des messages transformés A et B'.

Les figures 5 à 7 peuvent aussi servir pour illustrer le mode de réalisation dans lequel le représentant de l'autorité 3 est un microsystème informatique matériellement sécurisé, comprenant un dispositif d'interface 13. Le port d'entrée-sortie 10 du système d'interfaçage 7 est alors raccordé au dispositif d'interface 13.

La présente invention n'est pas limitée aux modes de réalisation qui ont été explicitement décrits, mais elle en inclut les diverses variantes et généralisations contenues dans le domaine des revendications ci-après.

REVENDICATIONS

1 - Procédé pour sécuriser les messages échangés sur un réseau de transmission de données entre un serveur (1) et un client (2) de petite taille et ne comportant pas en lui-même les ressources nécessaires pour remplir les fonctions de sécurité, sous le contrôle d'une autorité qui définit les règles d'échange des messages, caractérisé en ce que le contrôle est assuré de manière décentralisée par un représentant de l'autorité (3), intercalé en permanence dans le réseau à proximité du client (2) et entre le serveur (1) et le client (2) pendant l'échange sécurisé des messages, effectuant une traduction des messages transmis et effectuant sur les messages transmis les contrôles décidés par l'autorité.

2 - Procédé selon la revendication 1, caractérisé en ce qu'on utilise un premier protocole (P) pour les échanges entre le serveur (1) et le représentant de l'autorité (3), et on utilise un second protocole (P') différent du premier protocole (P) pour les échanges entre le représentant de l'autorité (3) et le client (2).

3 - Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que, pour l'échange de messages :
- on établit entre le serveur (1) et le représentant de l'autorité (3) un premier canal sécurisé (4) en utilisant une première clé (Ks) connue du représentant de l'autorité (3) et du serveur (1) mais pas du client (2), et en utilisant un premier algorithme de cryptage (AL),
- on établit entre le représentant de l'autorité (3) et le client (2) un second canal sécurisé (5) en utilisant une seconde clé (Kc) connue du représentant de l'autorité (3) et du client (2) mais pas du serveur (1), et en utilisant un second algorithme de cryptage (AL').

4 - Dispositif pour sécuriser les messages échangés sur un réseau de transmission de données entre un serveur (1) et un client (2) de petite taille et ne comportant pas en lui-même les ressources nécessaires pour remplir la fonction de sécurité, sous le contrôle d'une autorité qui définit les règles d'échange des messages, caractérisé en ce qu'il comprend un dispositif de contrôle décentralisé ou représentant de l'autorité (3), intercalé

en permanence dans le réseau à proximité du client (2) et entre le serveur (1) et le client (2) pendant l'échange sécurisé des messages, effectuant une traduction des messages transmis, et effectuant sur les messages transmis les contrôles décidés par l'autorité.

5 - Dispositif selon la revendication 4, caractérisé en ce que le dispositif de contrôle décentralisé ou représentant de l'autorité (3) est un microsystème informatique matériellement sécurisé, intercalé en permanence entre le serveur (1) et le client (2) pendant l'échange des messages.

6 - Dispositif selon la revendication 5, caractérisé en ce que :

- le serveur (1) est un système informatique comprenant un port d'entrée-sortie (1a) ;
- le client (2) est un microsystème informatique comprenant un port d'entrée-sortie (12) ;
- le représentant de l'autorité (3) est un microsystème informatique matériellement sécurisé comprenant un dispositif d'interface (13) ;
- un système spécifique d'interfaçage (7) est prévu, comprenant un port d'entrée-sortie (8) connecté au port d'entrée-sortie (1a) du système informatique serveur (1), comprenant un port de cartes (9) connecté au port d'entrée-sortie (12) du microsystème informatique client (2), comprenant un port d'entrée-sortie (10) connecté au dispositif d'interface (13) du microsystème informatique représentant l'autorité (3), et comprenant un contrôleur (11) programmé pour contrôler les communications entre les ports d'entrée-sortie (8), (9) et (10) ;
- le contrôleur (11) et le représentant de l'autorité (3) sont programmés de façon que :
  - le système informatique serveur (1) envoie une requête A au microsystème informatique client (2), et cette requête est reçue par le contrôleur (11) ;
  - le contrôleur (11) transmet la requête A au représentant de l'autorité (3), qui lui retourne une réponse Ra ;

- cette réponse Ra est utilisée par le contrôleur (11) pour calculer une requête A' qui est envoyée au microsystème informatique client (2) ;
- la requête A' est traitée par le microsystème informatique client (2), qui prépare une réponse B' ;
- le microsystème informatique client (2) envoie la réponse B' au système informatique serveur (1) ; cette réponse est reçue par le contrôleur (11) ;
- le contrôleur (11) transmet la réponse B' au représentant de l'autorité (3), qui lui retourne une réponse Rb ;
- cette réponse Rb est utilisée par le contrôleur (11) pour calculer une réponse B qui est envoyée au système informatique serveur (1).

7 - Dispositif selon la revendication 6, caractérisé en ce que :
- le client (2) est une carte à microprocesseur ;
- le représentant de l'autorité (3) est une carte à microprocesseur ;
- le système spécifique d'interfaçage est un lecteur de cartes à microprocesseur (7) comportant deux ports de cartes (9) et (10).

8 - Dispositif selon la revendication 6, caractérisé en ce que :
- le client (2) est un système mobile de communication ;
- le serveur (1) est un système informatique communiquant avec le client (2) par une connexion physique ou par un réseau de communication sans fil ;
- le représentant de l'autorité (3) est une carte à microprocesseur représentant l'opérateur du réseau de communication sans fil (dite carte SIM dans les téléphones répondant aux normes GSM).

9 - Dispositif selon la revendication 6, caractérisé en ce que :
- le client (2) est une carte à microprocesseur ;
- le représentant de l'autorité (3) est un système informatique matériellement sécurisé ;
- le système spécifique d'interfaçage (7) est une machine comportant un port de cartes (9) et une interface d'entrée-sortie

spécifique (10) de liaison avec le système informatique représentant de l'autorité (3).

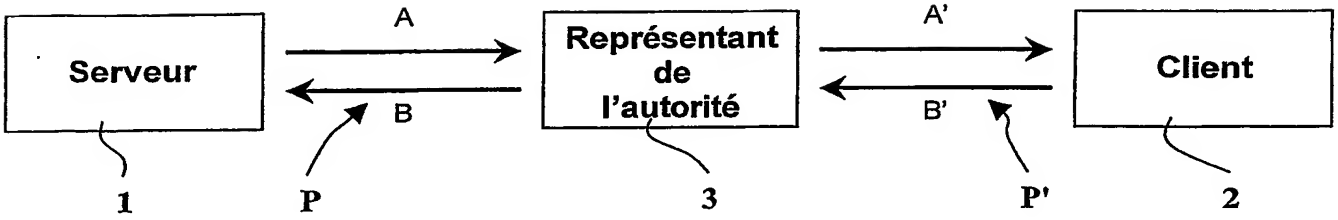


FIG. 1

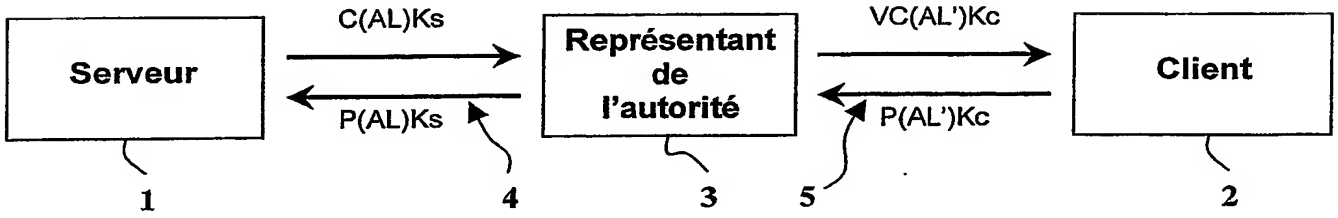


FIG. 2

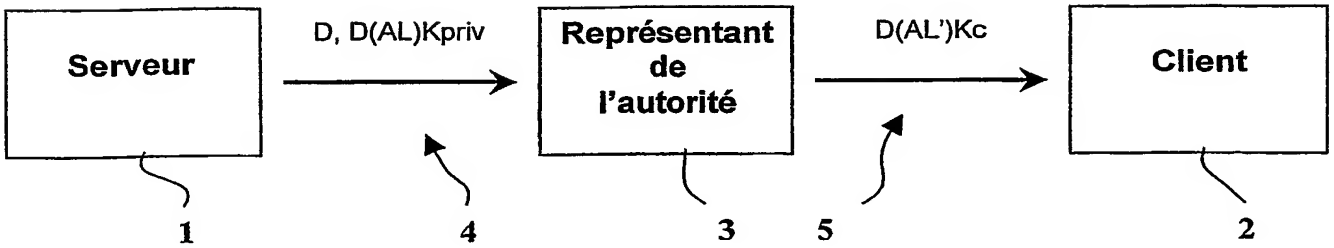


FIG. 3

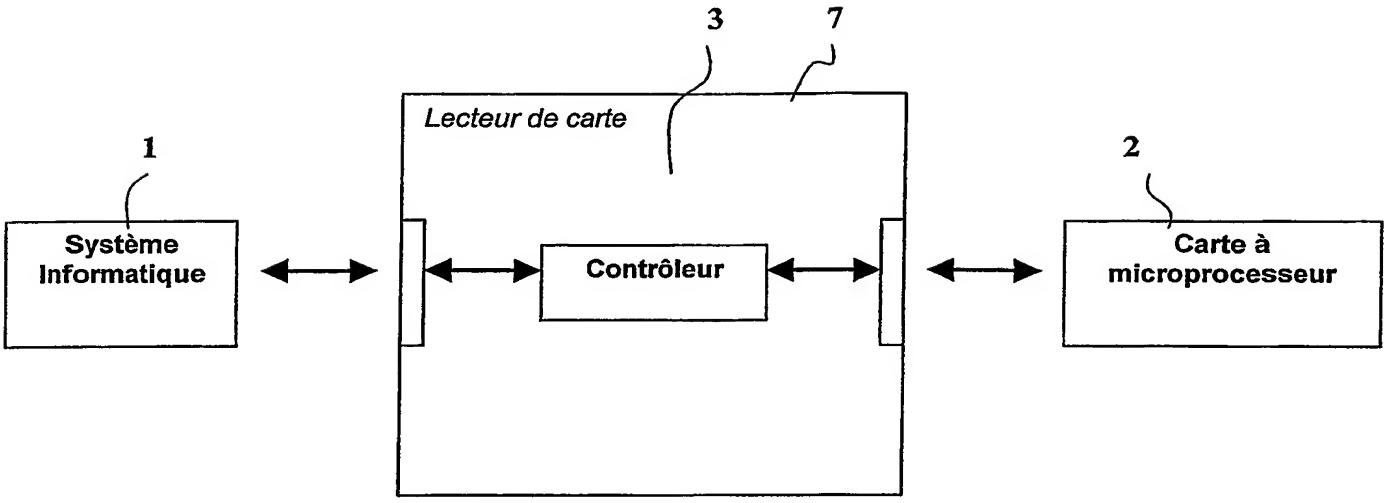

3
7
Lecteur de carte
1
2
Système Informatique
Contrôleur
Carte à microprocesseur

FIG. 4

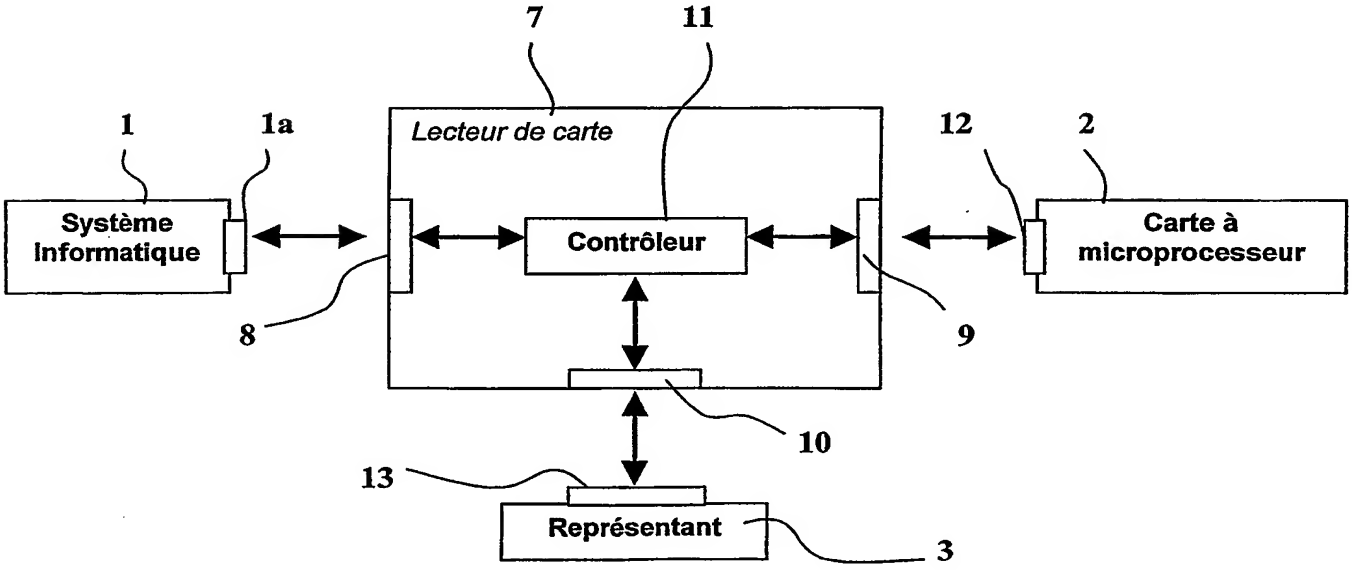

7
11
1
1a
Lecteur de carte
12
2
Système Informatique
Contrôleur
Carte à microprocesseur
8
9
10
13
Représentant
3

FIG. 5

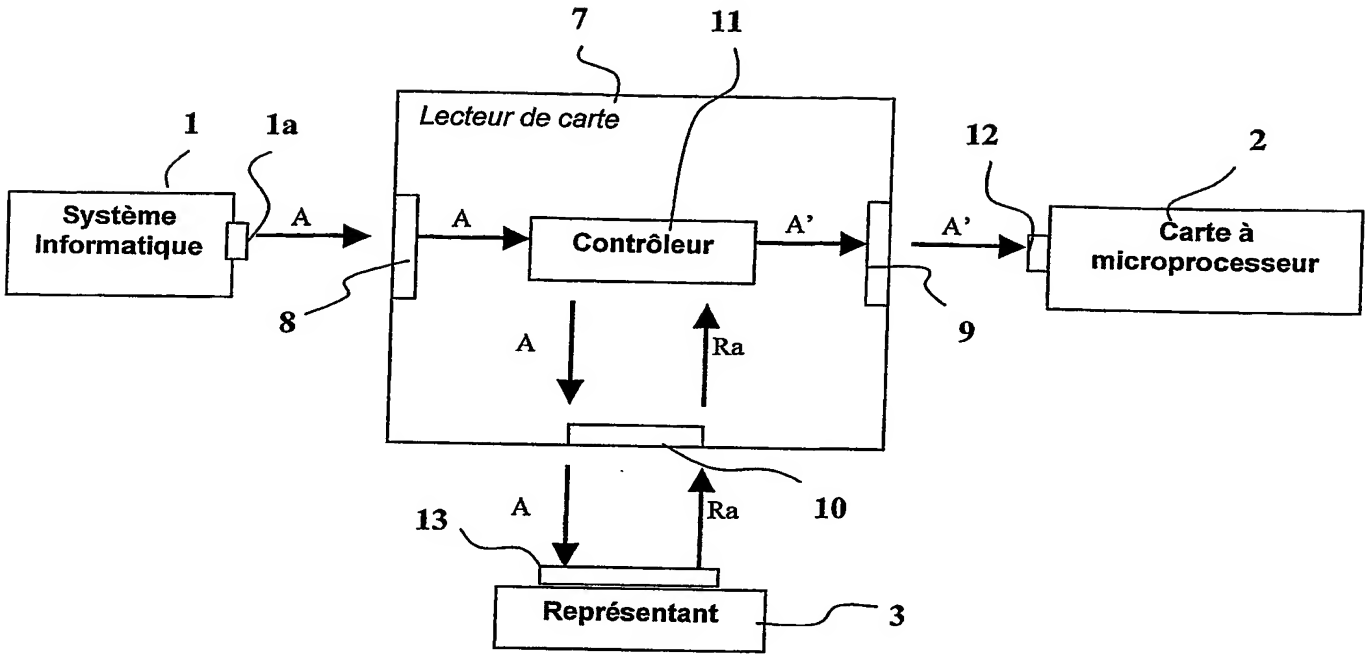

7
11
Lecteur de carte
1
1a
Système Informatique
A
A
Contrôleur
A'
A'
12
2
Carte à microprocesseur
8
9
A
Ra
10
13
A
Ra
Représentant
3

FIG. 6

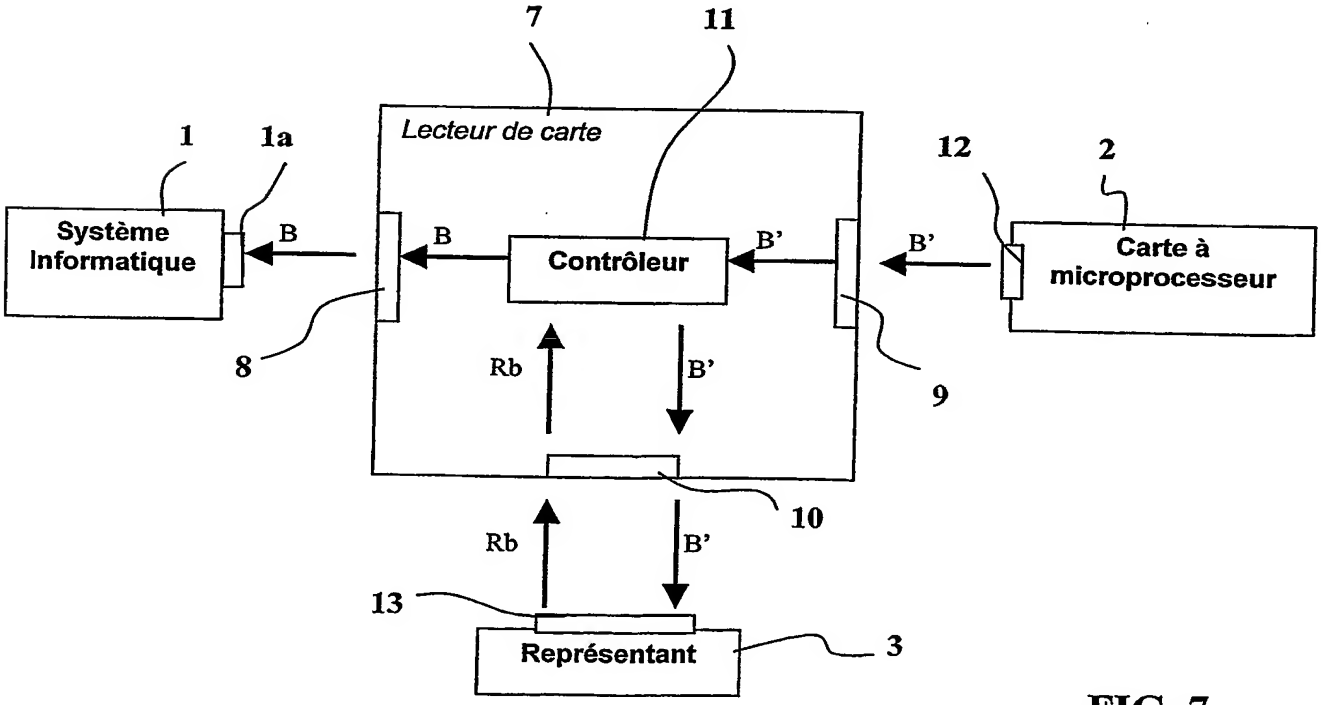

7
11
Lecteur de carte
1
1a
Système Informatique
B
B
Contrôleur
B'
B'
12
2
Carte à microprocesseur
8
9
Rb
B'
10
Rb
B'
13
Représentant
3

FIG. 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR [redacted]/00288

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L29/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DOMINGO-FERRER J ET AL: "Current directions in smart cards" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 36, no. 4, 16 July 2001 (2001-07-16), pages 377-379, XP004304903 ISSN: 1389-1286 abstract page 378, left-hand column, line 8 -right-hand column, line 30 --- -/--	1-9

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 July 2003	11/07/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Adkhis, F

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	URIEN P: "Internet card, a smart card as a true Internet node" COMPUTER COMMUNICATIONS, ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, NL, vol. 23, no. 17, 1 November 2000 (2000-11-01), pages 1655-1666, XP004238469 ISSN: 0140-3664 abstract page 1663, left-hand column, line 23 -right-hand column, line 36 page 1664, left-hand column, line 3 -page 1665, right-hand column, line 4	1-9

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 03/00288

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L29/06 H04L29/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	DOMINGO-FERRER J ET AL: "Current directions in smart cards" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 36, no. 4, 16 juillet 2001 (2001-07-16), pages 377-379, XP004304903 ISSN: 1389-1286 abrégé page 378, colonne de gauche, ligne 8 -colonne de droite, ligne 30 --- -/--	1-9

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
4 juillet 2003	11/07/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Adkhis, F

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	URIEN P: "Internet card, a smart card as a true Internet node" COMPUTER COMMUNICATIONS, ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, NL, vol. 23, no. 17, 1 novembre 2000 (2000-11-01), pages 1655-1666, XP004238469 ISSN: 0140-3664 abrégé page 1663, colonne de gauche, ligne 23 -colonne de droite, ligne 36 page 1664, colonne de gauche, ligne 3 -page 1665, colonne de droite, ligne 4	1-9